View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Southern Methodist University

Science and Technology Law Review

Volume 22 | Number 1 Article 5

2019

Corporate Genealogists: The New Homicide Detectives

Morgan Crider
Southern Methodist University, Dedman School of Law, mcrider@smu.edu

Follow this and additional works at: https://scholar.smu.edu/scitech

 Part of the Criminal Law Commons, and the Science and Technology Law Commons

Recommended Citation

Morgan Crider, *Corporate Genealogists: The New Homicide Detectives*, 22 SMU SCI. & TECH. L. REV. 153 (2019)
https://scholar.smu.edu/scitech/vol22/iss1/5

This Case Note is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.

Corporate Genealogists: The New Homicide Detectives

*Morgan Crider**

I. INTRODUCTION

On April 24, 2018, the Sacramento Police Department (SPD) revealed that they had used a commercial DNA database to identify a suspect whom they believed to be the "Golden State Killer."[1] The SPD was able to identify a familial match to the alleged killer by uploading DNA evidence obtained from crime scenes to the genealogical website, GEDMatch.[2] On GEDMatch, the SPD was able to compare the genetic profile from the evidence with profiles uploaded to the site by private users.[3] From there, the SPD created a family tree based on the ancestry of the genetic match and identified an individual who fit the profile of the Golden State Killer.[4] The SPD accessed the genealogy website as a private user, never obtaining a warrant to access the genetic information in an official law enforcement capacity.[5]

DNA has advanced to the point where law enforcement can now use genealogical profiles to construct family trees and identify criminal suspects based on their ancestry.[6] Traditionally, the databases used by authorities have been federal and state government originated, and subject to statutory regulations with respect to DNA entry and use.[7]

This Note analyzes law enforcement's use of commercial DNA databases—designed for private genealogical or diagnostic research—for criminal investigations.

---

* Morgan Crider is a 2020 candidate for Juris Doctor from SMU Dedman School of Law. She received a Bachelor of Agricultural Communications and Journalism from Texas A&M University in 2017.

1. *See* Thomas Fuller, *How a Genealogy Site Led to the Front Door of the Golden State Killer Suspect*, N.Y. TIMES (Apr. 26, 2018), https://www.nytimes.com/2018/04/26/us/golden-state-killer.html.

2. *See* Avi Selk, *The Ingenious and 'Dystopian' DNA Technique Police Used to Hunt the 'Golden State Killer' Suspect*, WASH. POST (Apr. 28, 2018), https://www.washingtonpost.com/news/true-crime/wp/2018/04/27/golden-state-killer-dna-website-gedmatch-was-used-to-identify-joseph-deangelo-as-suspect-police-say/?utm_term=.ed7e023c53b7.

3. *See id.*

4. *See id.*

5. *See id.*

6. *See id.*

7. *See* 34 U.S.C.A. § 40702 (West 2018).

II. GOVERNMENT DNA COLLECTION AND THE FOURTH AMENDMENT

During the past twenty-four years, law enforcement has actively sought to collect DNA from a large pool of individuals.[8] Considering these efforts, there has been both statutory and court guidance with respect to DNA collection and use.[9] Courts have repeatedly implied that genetic information is actual property protected under the Fourth Amendment.[10]

A. The Evolution of Government DNA Collection.

The Combined DNA Index System (CODIS) connects DNA laboratories on the national, state, and local levels in a centralized software system.[11] In 1994, Congress enacted the DNA Identification Act, which established the National DNA Index System (NDIS).[12] NDIS was created to stockpile DNA profile records entered by local, state, and federal law enforcement agencies as part of CODIS.[13] CODIS and NDIS are governed by statutory provisions and are supervised by the FBI.[14] The purpose of having a government-maintained DNA database is to allow "'State and local forensics laboratories to exchange and compare DNA profiles electronically in an attempt to link evidence from crime scene for which there are no suspects to DNA samples of convicted offenders on file in the system.'"[15]

The DNA collection begins with the Local DNA Index System (LDIS), where local laboratories take samples and use them to generate CODIS profiles.[16] At the second level, the State DNA Index System (SDIS), state law enforcement agencies input the LDIS information into their state-wide

8. *See id.* § 12592 (formerly cited as 42 U.S.C.A. § 14132 (West 1994)).

9. *See id.* § 40702(a)(1)(B).

10. *See* United States v. Kriesel, 720 F.3d 1137, 1144 (9th Cir. 2013); *see also* Maryland v. King, 569 U.S. 435, 446 (2013).

11. *See Combined DNA Index System (CODIS)*, FED. BUREAU OF INVEST., https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited Aug. 26, 2019).

12. *See id.*

13. *See id.*

14. *See id.* (codified in 34 U.S.C.A. § 12592).

15. United States v. Mitchell, 652 F.3d 387, 399 (3d Cir. 2011) (quoting H.R. REP. 106-900(I) (2000)).

16. *See* Stephen Mercer & Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. ANN. SURV. AM. L. 639, 650 (2014); *see also Combined DNA Index System (CODIS) Brochure*, FED. BUREAU OF INVEST. (2015), https://www.fbi.gov/file-repository/combined-dna-index-system-codis-brochure.pdf/view.

databases.[17] Lastly, at NDIS, the highest level, state profiles are uploaded into the national database but may be rejected if the FBI finds that the DNA profile does not meet the NDIS standard requirements.[18]

CODIS DNA profiles focus on the analysis of chromosomes in the nucleus of human cells, specifically, the DNA sequence unique to each human genome known as short tandem repeats (STRs).[19] The DNA profile will focus on alleles—the size and frequency of STRs along a strand of DNA—because the combination of alleles are analyzed to identify a single person.[20] As of August 2018, NDIS has 13,492,036 offender profiles, 3,246,832 arrestee profiles, and 879,945 forensic profiles.[21]

In contrast, familial DNA searches center on finding *common* alleles, not an identical profile match.[22] Closer genetic relationships, such as a parent and child, are likely to have a substantial number of allele commonalities.[23] Alternatively, distant genetic relationships result in fewer matching alleles which weaken the genetic profile's credibility.[24] According to the FBI, familial searching should be conducted for the sole purpose of identifying *close* biological relatives.[25] Further, familial DNA searches must be limited to relatives who are already in the DNA database.[26]

Familial DNA searches have frequently been met with criticism due to their over-inclusive results, and law enforcement's use of commercial genealogical databases have resulted in additional controversy.[27] Currently, familial searches are not performed on the national level, and familial searches are

17. *See* Mercer & Gabel, *supra* note 16, at 669.

18. *See id.*; *see also Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU OF INVEST., https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Aug. 26, 2019) (explaining that states may create their own standards for DNA collection, but contributions to NDIS must comply with federal provisions).

19. *See* Maryland v. King, 569 U.S. 435, 443 (2013).

20. *See id.*

21. *See CODIS-NDIS Statistics*, FED. BUREAU OF INVEST. (Aug. 2018), https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics.

22. *See* Jessica D. Gabel, *Probable Cause from Probable Bonds: A Genetic Tattle Tale Based on Familial DNA*, 21 HASTINGS WOMEN's L.J. 3, 11 (2010) (emphasis added).

23. *See id.*

24. *See id.*

25. *See Combined DNA Index System (CODIS)*, *supra* note 11.

26. *See id.*

27. *See* Justin Poulsen, *Your Relative's DNA Could Turn You Into a Suspect*, WIRED (Oct. 13, 2015), https://www.wired.com/2015/10/familial-dna-evidence-turns-innocent-people-into-crime-suspects; *see also* Selk, *supra*, note 2.

not conducted on NDIS.[28] Some states, such as Maryland and the District of Columbia, have statutorily prohibited the use of familial DNA testing, while other states, such as Texas, require approval from a review board before a familial search can be legally initiated.[29] Only Arkansas, California, Colorado, Florida, Michigan, Texas, Utah, Virginia, Wisconsin, and Wyoming permit familial DNA testing for criminal investigations.[30] There is considerable legislative concern regarding state use of familial DNA searches.[31] This concern should logically bleed over into the use of commercial genealogical databases by authorities to construct family trees. The FBI has distinguished genealogical searches from familial searches because the pool of DNA samples is from individuals who have submitted their DNA to third-party companies.[32] The key difference is that the DNA samples are not searched on government generated and regulated databases but instead on private commercial databases entitled to Fourth Amendment protections and free from federal oversight.[33]

B. Do You Have a Reasonable Expectation of Privacy to Your DNA?

An individual's DNA possesses unique information; however, the protection of that information from a warrantless intrusion is not absolute.[34] "[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[35] However, a Fourth Amendment search does not occur when an individual has not manifested a subjective expectation of privacy regarding the object of the search and society is unwilling to recognize that expectation as reasonable.[36] The touchstone of Fourth Amendment analysis is the reasonableness of the "governmental invasion of a citizen's personal security."[37] Reasonableness predominantly depends on the warrant clause, which requires authorities to

28. *See Combined DNA Index System (CODIS)*, *supra* note 11.

29. *See* Allison Murray et al., *Familial DNA Testing: Current Practices and Recommendations for Implementation*, 9 INVESTIGATIVE SCI. J., Sept. 8, 2017, at 1, 3.

30. *See Combined DNA Index System (CODIS)*, *supra* note 11.

31. *See* Michael B. Field et al., *Study of Familial DNA Searching Policies and Practices: Case Study Brief Series*, NAT'L CRIM. JUST. REFERENCE SERV. (Aug. 2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251081.pdf.

32. *See Combined DNA Index System (CODIS)*, *supra* note 11.

33. *See id.*

34. *See* Maryland v. King, 569 U.S. 435, 447 (2013); *see also* 34 U.S.C.A. § 40702(a)(1)(B).

35. Kyllo v. United States, 533 U.S. 27, 33 (2001).

36. *See id.*

37. *See* United States v. Kincade, 379 F.3d 813, 821 (9th Cir. 2004) (quoting Terry v. Ohio, 392 U.S. 1, 19 (1968)).

show probable cause to "a neutral magistrate" and persuade the magistrate to provide authorization to carry out a search by issuing authorities a warrant.[38] In some narrow circumstances, law enforcement may execute a search without a warrant so long as the search is reasonable, such as in searches conducted after a lawful arrest.[39]

In 2000, Congress authorized the DNA Act, which requires the collection of DNA samples from any individual "in the custody of the Bureau of Prisons who is, or has been, convicted of a qualifying federal offense."[40] Further, the DNA Act allows the collection of DNA samples "from individuals who are arrested, facing charges, or convicted from non-United States persons who are detained under the authority of the United States."[41]

The United States Supreme Court held in *Maryland v. King* that the police can reasonably collect a buccal DNA swab from an individual taken into police custody without a warrant because detainees have a diminished expectation of privacy.[42] The Supreme Court noted that traditionally, some indication of "individualized suspicion" as justification for a constitutional search or seizure was preferred, "[b]ut the Fourth Amendment imposes no irreducible requirement of such suspicion."[43] With respect to constitutional protection from search and seizure, the question is one of reasonableness.[44] Courts must consider the special needs of law enforcement and weigh those interests against an individual's right to a reasonable expectation of privacy.[45] In its holding, the Supreme Court reasoned that an individual taken into police custody has a diminished expectation of privacy compared to a citizen who has not been suspected of wrongdoing.[46] By distinguishing individuals in police custody from those who are not, the Supreme Court implies that the police must obtain a warrant to collect DNA from individuals whom the police do not possess sufficient suspicion to arrest.

III. COMMERCIAL GENEALOGY TURNED INVESTIGATIVE TOOL

The Supreme Court posed the notion that the necessity of a warrant is at its minimum when the search "involves no discretion that could properly be

38. *See id.* at 822 (citing United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div., 407 U.S. 297, 315 (1972)).

39. *See id.*

40. 34 U.S.C.A. § 40702(a)(1)(B).

41. *See id.* § 40702(a)(1)(A).

42. *See* Maryland v. King, 569 U.S. 435, 447 (2013).

43. *See id.*

44. *See id.*

45. *See id.* at 447, 461.

46. *See id.* at 463–464.

limited" by the actions of a neutral third-party between the citizen whose DNA is being collected and law enforcement;[47] "it would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[48] Law enforcement takes this concept to heart by accessing a commercial genealogical database, "a neutral third-party," as a private user to identify the DNA sample needed in an investigation.[49]

Genealogy companies such as Ancestry.com and 23andMe, in their terms of service, explain that the genetic information sent to them is in some form preserved by the company.[50] GEDMatch's user policies state:

> We may disclose your Raw Data, personal information, and/or Genealogy Data if it is necessary to comply with a legal obligation such as a subpoena or warrant. We will attempt to alert you to this disclosure of your Raw Data, personal information, and/or Genealogy Data, unless notification is prohibited under law.[51]

This use and preservation of genetic information, whether in the form of property rights or licensing agreements, classifies the information as being within the possession of the genealogy companies, which warrants Fourth Amendment protection.[52]

In the case of the Golden State Killer, the SPD did not obtain a warrant when it accessed the commercial genealogy site as a private user.[53] During its investigation, the SPD utilized GEDMatch's resources to identify suspects.[54] This access to voluntarily submitted DNA is distinguishable from an arrestee, or pretrial detainee, being required to provide DNA by law enforcement, as permitted under 34 U.S.C.A. § 40702, because police are accessing this information without a warrant and § 40702 neither expressly nor implicitly permits the collection of DNA from a commercial corporation's resources without a warrant.[55]

---

47. *See id.* at 447.

48. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that sensitive information gathered through an unprecedented use of technology constituted a "search" which required a warrant).

49. *See* Selk, *supra* note 2.

50. *See Ancestry Terms and Conditions*, ANCESTRY.COM (June 5, 2018), https://www.ancestry.com/cs/legal/termsandconditions; *see also Terms of Service*, 23ANDME, https://www.23andme.com/about/tos (last visited Aug. 26, 2019).

51. *See GEDMatch.com Terms of Service and Privacy Policy*, GEDMATCH (May 20, 2018), https://www.gedmatch.com/tos.htm.

52. *See* Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920).

53. *See* Selk, *supra* note 2.

54. *See id.*

55. *See* 34 U.S.C.A. § 40702 (West 2018).

In contrast, this kind of access *is* analogous to the government unlawfully seizing assets from a business because, as stated in *United States v. Kriesel*, genetic information such as blood may be considered property.[56] Law enforcement is still required to follow the guidelines of the Fourth Amendment with respect to the seizure of such company assets, even if the assets consist of genetic information, until there is a statutory provision stating otherwise.[57] Moreover, in instances where companies, such as GEDMatch, will only share its resources with law enforcement under a legal obligation stemming from a subpoena or warrant, the authorities' presentation of itself as a consumer could be considered fraudulent.[58]

Similarly, Apple has fought the government with respect to law enforcement's use of the company's technology in criminal investigations, even with the presence of a warrant, because of the severe implications of iPhone users' diminished expectation of privacy.[59] Further, fourteen major technology companies, including Google and Verizon, signed onto an amicus brief submitted to the Supreme Court in response to the privacy issues raised in *United States v. Carpenter*.[60] The brief asserted that the users of the amici's technological services do not necessarily expect their information, shared through their normal use of the services, to be available to law enforcement without a warrant.[61] There is still a reasonable expectation of privacy with respect to information that becomes a commercial company's property.[62] "When law-enforcement agencies seek user data pursuant to a warrant . . . [the technology companies] work to ensure that investigative needs are met

56. United States v. Kriesel, 720 F.3d 1137, 1144 (9th Cir. 2013)

57. *See Silverthorne Lumber*, 251 U.S. at 392.

58. However, this is considered unlikely given that this use is similar to law enforcement creating fake Facebook profiles to target suspects, a practice courts have upheld. *See* Christina Sterbenz, *Cops are Creating Totally Bogus Facebook Profiles Just so they Can Arrest People*, BUS. INSIDER (Oct. 21, 2013), https://www.businessinsider.com/police-make-fake-facebook-profiles-to-arrest-people-2013-10; *see also* Sari Horwitz, *Justice Dept. Will Review Practice of Creating Fake Facebook Profiles*, WASH. POST (Oct. 7, 2014), https://www.washingtonpost.com/world/national-security/justice-dept-will-review-practice-of-creating-fake-facebook-profiles/2014/10/07/3f9a2fe8-4e57-11e4-aa5e-7153e466a02d_story.html?utm_term=.06657d71ff7f.

59. *See In re* Apple Motion to Vacate, at 1, Matter of Search of an Apple iPhone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016) (N.D. Cal.) (filed and settled outside of court).

60. Brief for Technology Companies as Amici Curiae in Support of Neither Party at 1–9, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16–402).

61. *See id.* at 18–20.

62. *See Silverthorne Lumber*, 251 U.S. at 392.

without subjecting users to undue intrusion."[63] These private companies emphasize that the presence of a warrant, and an opportunity to contest the seizure of such information, is key, as opposed to baseless searches with no reasonable limitations.[64] The technology companies "agree that Fourth Amendment doctrine should recognize that, in the evolving digital era, where such data is disclosed . . . people reasonably expect that their data will be stored securely and remain private."[65] There is a "societal understanding that certain areas," such as the digital realm, "deserve the most scrupulous protection from government invasion."[66]

The United States Supreme Court affirmed these companies' notion that the information they acquire through customers' use of their services warrant protection in the case of *Carpenter v. United States*.[67] Law enforcement's access to locational information collected by wireless carriers was found to require a warrant, which would limit the scope of a search.[68] The Supreme Court stated that while the standard for searches may be reasonableness, case law has established that warrantless searches are typically unreasonable where "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing."[69] A warrant is required where an individual has a "legitimate privacy interest" in information managed by third-party entities.[70] The government's ability to access information that is normally guarded has progressed with technology, and the Supreme Court "has sought to 'assure the preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' "[71]

The notion of corporate asset protection is contended to be worthy of an even higher standard, as Apple argued with respect to its customers' iPhone privacy.[72] In the case of the San Bernardino, California mass shooting, the FBI filed suit to compel Apple to unlock an encrypted iPhone used by one of the two attackers after Apple adamantly opposed disclosing the information

63. *See* Brief for Technology Companies as Amici Curiae in Support of Neither Party at 20, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16–402).

64. *See id.* at 11, 21.

65. *See id.* at 1.

66. *See id.* at 22 (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)).

67. *See* 138 S. Ct. 2206, 2210–11 (2018).

68. *See id.* at 2210–11 (2018).

69. *See id.* at 2221.

70. *See id.* at 2222.

71. *See id.* at 2214 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

72. *See* Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 2, Matter of Search of an Apple iPhone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016) (No. ED 15–0451M).

as an invasion of the iPhone user's reasonable expectation of privacy by creating a security vulnerability in iPhones.[73] After a United States District Court in California ordered Apple to unlock the encrypted iPhone, Apple's counsel filed a petition to vacate the order, asserting that "[c]ompelling Apple to create software [to unlock an individual iPhone] will set a dangerous precedent for conscripting Apple and other technology companies to develop technology to do the government's bidding in untold future criminal investigations."[74] These sentiments are echoed in the *Carpenter* amicus brief, emphasizing the sensitivity of the data entrusted to them, which requires that companies who use information to provide services must work to protect customer information and take "substantial measures to honor and reinforce their customers' expectation of privacy."[75]

Ancestry.com (Ancestry) publishes an annual transparency report, accessible to its users (members), which covers law enforcement requests for member information.[76] Ancestry requires valid legal process in order to produce information about its members, and it only complies with legitimate requests, such as subpoenas and warrants.[77] When Ancestry receives a legal request for information concerning its members, Ancestry officials review the request to ensure it satisfies legal requirements and will attempt to narrow the disclosure if Ancestry believes the request is overly broad.[78] There is a clear threat with respect to an unlimited access to commercial genealogy databases, and Ancestry has acted preemptively to counter that threat.

As biometrics become a prominent aspect for private businesses, authorities are more likely to lean on these companies for access to their unwitting consumers' genetic information. Police have become consumers rather than producers of surveillance.

IV. TESTING QUALITY VERSUS QUANTITY

Commercial genealogical databases are not held to the same standard as government-regulated DNA databases and are therefore more susceptible egregious errors.[79] During the SPD's investigation into the Golden State

73. *See id.* at 7.

74. *See id.* at 25.

75. *See* Brief for Technology Companies as Amici Curiae in Support of Neither Party at 20, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16–402).

76. *See Your Privacy*, ANCESTRY.COM (Apr. 30, 2018), https://www.ancestry.com/cs/legal/privacystatement.

77. *See Ancestry 2018 Transparency Report*, ANCESTRY.COM (2018), https://www.ancestry.com/cs/transparency.

78. *See Ancestry Guide for Law Enforcement*, ANCESTRY.COM, https://www.ancestry.com/cs/legal/lawenforcement (last visited Aug. 8, 2019).

79. *See Regulation of Genetic Tests*, NAT'L HUMAN GENOME RES. INST. (Jan. 17, 2018), https://www.genome.gov/10002335/regulation-of-genetic-tests; *see also*

Killer, the department initially misidentified a man from Oregon as the suspect because of a similar but tenuous genetic connection to the SPD's reconstructed family tree taken from GEDMatch.[80]

Similarly, in 2015, law enforcement in Idaho relied on a potential familial genetic match from a commercial genealogy company, leading to the misidentification of man in a murder investigation.[81] Michael Usry became a suspect in the 1996 murder investigation of a woman from Idaho Falls.[82] He had been identified as one of three potential suspects after law enforcement ran a familial search through a genetic database from Ancestry.com.[83] The police had received a court order to compel Ancestry.com to give the detectives access to its DNA database, some of which the company obtained from a genealogy project conducted by a Mormon Church that Usry's father had participated in.[84]

For a local laboratory to contribute to CODIS, "the lab must sign a memorandum of understanding agreeing to adhere to the quality standards and submit to audits to evaluate compliance with federal standards for scientifically rigorous DNA testing."[85] In general, laboratories seeking to participate in NDIS need to be accredited in DNA by a nonprofit professional association involved in and nationally recognized by the forensic science community.[86]

Commercial genealogy and genetic businesses such as 23andMe offer to test DNA samples and provide individualized reports on genetic conditions, ranging from those genes associated with serious health disorders to those associated with hair loss and food preferences.[87] Unlike government-based DNA databases, commercial genealogical businesses do not face the same

---

NDIS Operational Procedures Manual, FED. BUREAU OF INVEST. (2018), https://www.fbi.gov/file-repository/ndis-operational-procedures-manual.pdf/view.

80. *See* Selk, *supra* note 2.

81. *See* Poulsen, *supra* note 27; *see also* Jim Mustian, *New Orleans Filmmaker Cleared in Cold-Case Murder; False Positive Highlights Limitations of Familial DNA Searching*, NEW ORLEANS ADVOC. (Mar. 12, 2015), https://www.theadvocate.com/new_orleans/news/article_1b3a3f96-d574-59e0-9c6a-c3c7c0d2f166.html.

82. *See* Poulsen, *supra* note 27.

83. *See* Mustian, *supra* note 81.

84. *See* Poulsen, *supra* note 27.

85. *See* Maryland v. King, 569 U.S. 435, 445 (2013).

86. *See NDIS Operational Procedures Manual*, *supra* note 79, § 2.1.

87. *See* Erin Murphy, *DNA in the Criminal Justice System: A Congressional Research Service Report* (*from the Future)*, 64 UCLA L. REV. DISC. 340, 344 (2016).

level of regulation with respect to their DNA testing.[88] The most common test kits are "laboratory-developed tests" (LDTs), where the test is created and tested by a single laboratory and where genetic samples are to be sent.[89] Genealogical and genetic companies are only under the regulatory "enforcement discretion" of the U.S. Food and Drug Administration (FDA) in terms of commercial DNA testing.[90] Enforcement discretion means that the FDA has the authority to regulate the test, but it chooses not to.[91] Therefore, LDTs are used without the FDA's certification with respect to the test's analytical and clinical validity.[92]

Further, ancestry test results are not necessarily consistent across different providers.[93] Commercial genealogy companies may come to different conclusions with respect to the percentage of ancestry from a particular region, because the results are largely dependent on the quality of the samples and the diversity of the genetic pool to which the samples are being compared.[94] DNA ancestry companies use reference databases to infer an individual's ancestry, and each company has its own database to determine ancestry according to geographical location, called Ancestry Informative Markers (AIMs).[95] AIMs are developed from databases of Single Nucleotide Polymorphisms (SNPs), and the ancestry results depend on the number of AIMs used.[96] Because each company has its own AIM, the results for ancestry are not necessarily the same.[97]

In 2017, the FDA released a discussion paper with suggested guidelines for the regulation of commercial genealogy companies because of the increased demand for direct-to-consumer genomic testing and advances in next-generation sequencing technology, which, without regulation, would

88. *See Regulation of Genetic Tests*, *supra* note 79.

89. *See id.*

90. *See id.*

91. *See id.*

92. *See id.*

93. *See* Kira Peikoff, *I Had My DNA Picture Taken, With Varying Results*, N.Y. TIMES (Dec. 30, 2013), https://www.nytimes.com/2013/12/31/science/i-had-my-dna-picture-taken-with-varying-results.html?_r=0 (explaining that genetic testing companies read segments of DNA to identify traits, diseases, etc., and different companies may read different segments of the same DNA sample).

94. *See* Sheldon Krimsky & David Cay Johnston, *Ancestry DNA Testing and Privacy: A Consumer Guide*, COUNCIL FOR RESPONSIBLE GENETICS (Mar. 2017), http://www.councilforresponsiblegenetics.org/img/Ancestry-DNA-Testing-and-Privacy-Guide.pdf.

95. *See id.*

96. *See id.*

97. *See id.*

pose a public health threat.[98] However, the discussion paper was simply the FDA's current thoughts on the topic, so it is not legally binding. In the discussion paper, the FDA stated that it would not issue final guidance on oversight for LDTs until there had been further public discussion and legislative guidance on the subject.[99]

Law enforcement is using a resource originally created for profit that was not required to meet the same regulatory standard as the CODIS.[100] The federal statutory provisions governing CODIS are there to ensure that no private citizen is wrongfully deprived of his or her freedom. Allowing potentially low-quality evidence to be searched in unregulated databases casts a wide net of suspicion over a vast amount of people. In a situation such as the Golden State Killer investigation, there is a degradation of standards in DNA testing and unfettered government access to a commercial corporation's resources disguised as a private consumer search.[101]

V. REINFORCING PRIVACY AND RAISING THE STANDARD

If the use of commercial genealogical databases is to be commonplace, there must be explicit legislation to permit law enforcement to act without a warrant in using commercial resources for DNA collection. DNA possesses a plethora of information as unique to individuals as locational information, which was deemed worthy of a warrant in *Carpenter v. United States*.[102] Additionally, considering the vast number of people within these commercial databases and the tenuous science of familial searches, there needs to be a clearly defined scope to these searches.

Further, if these corporate assets are to be used in the most serious of investigations, then the DNA testing from these commercial laboratories should be held to a higher standard that is more akin to that of a lab worthy of NDIS admission. Absent this level of scrutiny, and without proper regulation of DNA testing used by law enforcement, such reliance on questionable resources could result in a back-step in the use of DNA evidence.

98. *See id.*

99. *See Regulation of Genetic Tests*, *supra* note 79; *see also Discussion Paper on Laboratory Developed Tests (LDTs)*, U.S. Food & Drug Admin. (Jan. 13, 2017), https://www.fda.gov/downloads/medicaldevices/productsandmedicalprocedures/invitrodiagnostics/laboratorydevelopedtests/ucm536965.pdf.

100. *See* Selk, *supra* note 2; *see also Regulation of Genetic Tests*, *supra* note 79.

101. *See* Fuller, *supra* note 1.

102. 138 S. Ct. 2206, 2210 (2018).